UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,223	08/16/2001	Thomer Michael Gil	RIV-0440	2855

87555 7590 07/15/2009

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
NAWAZ, ASAD M	

ART UNIT	PAPER NUMBER
2455	

MAIL DATE	DELIVERY MODE
07/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte THOMER MICHAEL GIL,
MASSIMILIANO ANTONIO POLETTO,
and EDWARD W. KOHLER JR.

Appeal 2008-006300
Application 09/931,223
Technology Center 2400

Decided:[1] July 15, 2009

Before JOHN A. JEFFERY, ST. JOHN COURTENAY III,
and STEPHEN C. SIU, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-21 and 50-77.[2] We have jurisdiction under 35 U.S.C. § 6(b).[3] We reverse.

STATEMENT OF THE CASE

Appellants invented a system for thwarting denial of service attacks on a victim data center. Specifically, network traffic flow is monitored and statistics are produced according to a parameter of the traffic flow. The traffic flow is mapped into plural buckets, the number of which is varied according to the amount of traffic and number of flows. Accumulated statistics are then analyzed to identify the source of the attack. By dynamically varying the number of buckets, the monitoring process is not vulnerable to a denial of service attack against its own resources.[4] Claim 63 is illustrative:

63. A method of monitoring traffic flow in a monitor device disposed to receive network packets, the method comprises:

producing statistics corresponding to a parameter of the traffic flow to trace a source of an attack, with producing further comprising:

mapping the traffic flow into a plurality of buckets;

---

[2] The Examiner withdrew a rejection under 35 U.S.C. § 112. *See* Ans. 11; *see also* Reply Br. 1. Accordingly, that rejection is not before us.

[3] Appellants waived appearance at an oral hearing scheduled for this appeal on July 9, 2009. *See* Communication filed June 8, 2009.

[4] *See generally* Spec. 1-3, 14, and 15; Figs. 7 and 8.

varying the number of buckets according to the amount of traffic and number of flows to breakdown traffic flow into different buckets; and

analyzing statistics accumulated for a parameter and a corresponding threshold in the bucket to identify the source of the attack.

The Examiner relies on the following as evidence of unpatentability:

Hsu	US 6,098,157	Aug. 1, 2000
Lyle	US 6,971,028 B1	Nov. 29, 2005 (filed July 14, 2000)

1. The Examiner rejected claims 63-68 and 70-75 under 35 U.S.C. § 102(e) as anticipated by Lyle. Ans. 3-6.
2. The Examiner rejected claims 1-21, 50-62, 69, 76, and 77 under 35 U.S.C. § 103(a) as unpatentable over Lyle and Hsu. Ans. 6-10.

Rather than repeat the arguments of Appellants or the Examiner, we refer to the Briefs and the Answer[5] for their respective details. In this decision, we have considered only those arguments actually made by Appellants. Arguments which Appellants could have made but did not make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

[5] Throughout this opinion, we refer to (1) the Appeal Brief filed August 30, 2007; (2) the Examiner's Answer mailed July 3, 2007; and (3) the Reply Brief filed August 30, 2007.

THE ANTICIPATION REJECTION

Regarding independent claims 63 and 70, the Examiner finds that Lyle discloses all of the claimed subject matter including mapping traffic flow into plural "buckets" which the Examiner equates to Lyle's event data. *See* Ans. 3-5. *See also* Ans. 12 ("These traffic flows [corresponding to suspicious data] are placed in *events or buckets* and are placed in queues for further analysis.") (emphasis added). According to the Examiner, the number of these "buckets" or events are varied according to the amount of traffic since Lyle creates new events to accommodate new incidents as traffic increases. Ans. 13. The Examiner adds that the recited variation in the number of buckets is met since events and flows received close in time in the same network are accounted for when creating, dividing, or aggregating events. *Id.*

Appellants argue that Lyle does not vary the number of buckets according to the amount of traffic and number of flows as claimed, nor does Lyle examine statistics accumulated for a parameter and a corresponding threshold in the bucket as claimed. App. Br. 12-13; Reply Br. 4-7. Appellants emphasize that Lyle puts events into queues for processing events one at a time, and merely associates related events but does not combine such events. Reply Br. 6-7.

The issue before us, then, is as follows:

ISSUE

Under § 102, have Appellants shown that the Examiner erred in rejecting claims 63 and 70 by finding that Lyle (1) maps traffic flow in

plural buckets; (2) varies the number of buckets according to the amount of traffic and the number of flows to break down traffic flow in different buckets; and (3) analyzes statistics accumulated for a parameter and a corresponding threshold in the bucket to identify a source of an attack as claimed?

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence:

1. Lyle discloses a system for detecting and processing attacks on a computer network. Specifically, a "sniffer" module 304 continuously scans data received at various ports and identifies messages related to known or suspected attacks. Lyle, Abstract; col. 7, ll. 3-12 and 20-31; Fig. 3.

2. When information related to an actual or suspected attack is identified by the sniffer module (or received by handoff receiver 302), the information is sent to event manager 306 which places the suspicious data (i.e., "event data") in a queue and provides data to the analysis framework module 308 for processing, one event at a time, at predetermined intervals. The event manager also sends event data to the log database 320 for post-attack analysis. Lyle, col. 7, ll. 43-58; Fig. 3.

3. Analysis framework 308 (1) processes event data; (2) determines the appropriate course of action; and (3) takes the responsive action, if any. To this end, the analysis framework associates the event data with an event software object. The analysis framework also determines whether an event is associated with an existing event or group of related events and, if so,

associates related events into a single incident software object. Unrelated events, however, are associated with a new incident object. Lyle, col. 7, l. 59 – col. 8, l. 4; col. 13, ll. 19-61; Figs. 3 and 7.

4. An event software object stores event data and related data and can perform certain functions and processes either on or with respect to the event data. Lyle, col. 13, ll. 24-27.

5. Events may be aggregated into an existing incident based on similarities in the type of message and/or the target or destination address, or the presence of other strings or information indicated that the events are related. Lyle, col. 13, ll. 39-43.

6. Events that do not bear similarities may be aggregated into a single incident if the messages associated with the events are received close in time in the same network or sub-network. Lyle, col. 13, ll. 43-50; Fig. 7.

7. If an event is related to an existing incident, the event object is associated with an existing incident object. Otherwise, a new incident object is created and the event object is associated with the new incident object. Lyle, col. 13, ll. 51-58; Fig. 7.

8. Appellants' Specification indicates that "[t]he buckets are implemented as storage areas in the memory space of the data collector or gateway device." Spec. 14:16-18.

PRINCIPLES OF LAW

Anticipation is established only when a single prior art reference discloses, expressly or under the principles of inherency, each and every element of a claimed invention as well as disclosing structure which is

capable of performing the recited functional limitations. *RCA Corp. v. Appl. Dig. Data Sys., Inc.*, 730 F.2d 1440, 1444 (Fed. Cir. 1984); *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554 (Fed. Cir. 1983).

ANALYSIS

Claims 63 and 70 call for, in pertinent part, (1) mapping traffic flow in plural buckets; (2) varying the number of buckets according to the amount of traffic and the number of flows to break down traffic flow in different buckets; and (3) analyzing statistics accumulated for a parameter and a corresponding threshold in the bucket to identify a source of an attack.

We begin by construing the term "bucket." According to Appellants' Specification, "[t]he buckets are implemented as storage areas in the memory space of the data collector or gateway device." FF 8. As such, the Examiner's equating "events" with buckets that are placed in queues (Ans. 12) is problematic. While we can envision a queue as involving storage areas in the memory space of the event manager (and therefore reasonably constitute a "bucket") (*see* FF 2), this interpretation is inconsistent with the Examiner's analysis which is based on the event processing functionality of the *analysis framework*—not the event manager. *See* FF 8. This inconsistency is further illuminated by the fact that the event manager provides event data to the analysis framework one event at a time (FF 2)—a fact that would be inconsistent with varying the number of buckets at the event manager.

As such, based on the Examiner's analysis (Ans. 3, 4, 13), the Examiner apparently intends to equate the recited "buckets" with Lyle's event and incident objects that are created by the analysis framework. *See* FF 3-7. But even assuming that this is the case, the Examiner's reasoning is not persuasive.

That said, we can envision an event software object as reasonably constituting a "bucket" since the object stores event data and can perform certain functions associated with that data. *See* FF 4. Nevertheless, we still fail to see how the number of such buckets is varied according to (1) the amount of traffic, and (2) the number of flows to break down traffic into different buckets, let alone analyze statistics accumulated for a parameter and a corresponding threshold in the bucket as claimed.

Lyle does indicate that events are "aggregated" into single incident objects based on the presence of certain information associated with the event (FF 5), or if the messages are received close in time (FF 6). Nevertheless, this aggregation merely *associates* event objects with an incident object based on the specified conditions (FF 5-7): there is nothing in Lyle that indicates that the number of event objects (or incident objects) are necessarily varied in accordance with (1) the amount of traffic, and (2) the number of flows as claimed. The fact that events can be aggregated into a single incident (i.e., associated with a single incident object) based on their reception close in time (FF 6) simply does not cure this deficiency. The Examiner's position to the contrary (Ans. 13) is therefore unavailing.

For the foregoing reasons, Appellants have persuaded us of error in the Examiner's rejection of independent claims 63 and 70. Therefore, we will not sustain the Examiner's rejection of those claims, and dependent claims 64-68 and 71-75 for similar reasons.

THE OBVIOUSNESS REJECTION

Regarding independent claims 1, 14, and 21, the Examiner finds that Lyle discloses all of the claimed subject matter except for using a hash function to output an integer corresponding to one of the buckets. The Examiner, however, relies on Hsu for teaching this feature in concluding the claims would have been obvious. Ans. 6-10.

Appellants argue that the prior art does not teach or suggest, among other things, comparing the number of buckets to a threshold and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold as claimed in claim 1. App. Br. 17-20. Appellants further contend that the prior art does not teach or suggest adjusting the number of buckets as the number of buckets approaches a second threshold as claimed. App. Br. 26-27.

The issues before us, then, are as follows:

ISSUES

Under § 103, have Appellants shown that the Examiner erred in finding that Lyle and Hsu collectively teach or suggest:

(1) comparing the number of buckets to a threshold, and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold as recited in claim 1; and

(2) comparing the accumulated statistic values from the buckets to threshold values corresponding to the number of buckets to determine that an event is of significance, and adjusting the number of buckets as that number approaches a second threshold as recited in claims 14 and 21?

FINDINGS OF FACT

The record supports the following additional findings of fact (FF) by a preponderance of the evidence:

9. Hsu discloses a table located in a computer memory that is used to compile statistical information related to the quantity and size of data packets traveling on a LAN. The table is subdivided into buckets that are indexed by a unique identifier. Preferably, the unique identifier is the resulting value obtained from hashing address identifiers using a conventional hashing algorithm. Hsu, col. 5, ll. 5-24.

PRINCIPLES OF LAW

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so

doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966) (noting that 35 U.S.C. § 103 leads to three basic factual inquiries: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art). Furthermore, the Examiner's obviousness rejection must be based on

> "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" . . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.

KSR Int'l Co. v. Teleflex, Inc., 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

If the Examiner's burden is met, the burden then shifts to the Appellants to overcome the prima facie case with argument and/or evidence. Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments. *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

ANALYSIS

We will not sustain the Examiner's obviousness rejection of independent claims 1, 14, and 21. Claim 1 calls for, in pertinent part, comparing the number of buckets to a threshold, and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold.

As we indicated previously, although Lyle aggregates events into single incident objects based on the presence of certain information associated with the event (FF 5), or if the messages are received close in time (FF 6), Lyle does not teach varying the number of event objects (or incident objects) based on comparing the number of buckets to a threshold as claimed. Nor does Hsu cure this deficiency. *See* FF 9. Accordingly, we cannot sustain the Examiner's rejection of independent claim 1 or dependent claims 2-13 for similar reasons. Nor does Hsu cure the deficiencies we noted previously with respect to independent claims 63 and 70. As such, we cannot sustain the Examiner's rejection of dependent claims 69 and 76.

We likewise will not sustain the Examiner's rejection of claims 14 and 21 which call for, in pertinent part, comparing the accumulated statistic values from the buckets to threshold values corresponding to the number of buckets to determine that an event is of significance, and adjusting the number of buckets as that number approaches a second threshold. Our previous discussion regarding the shortcomings of Lyle applies equally here. For the reasons discussed previously, Lyle does not teach nor suggest these limitations, nor does Hsu cure this deficiency.

For the foregoing reasons, Appellants have persuaded us of error in the Examiner's rejection of independent claims 14 and 21. Therefore, we will not sustain the Examiner's rejection of those claims, and dependent claims 15-20, 50-62, and 77 for similar reasons.

CONCLUSION

Appellants have shown that the Examiner erred in rejecting (1) claims 63-68 and 70-75 under § 102, and (2) claims 1-21, 50-62, 69, 76, and 77 under § 103.

ORDER

The Examiner's decision rejecting claims 1-21 and 50-77 is reversed.

REVERSED

pgc

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis CA 95618